UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/068,889	02/11/2002	Francis Flanagan	P66398US1	4572

136 7590 09/07/2005

JACOBSON HOLMAN PLLC
400 SEVENTH STREET N.W.
SUITE 600
WASHINGTON, DC 20004

EXAMINER	
FIELDS, COURTNEY D	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 09/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/068,889	FLANAGAN ET AL.	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 February 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *07 May 2002*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-19 are pending.

Information Disclosure Statement

2. The Information Disclosure Statement respectfully submitted on 07 May 2002 have been fully considered by the Examiner.

Specification

3. The disclosure is objected to because of the following informalities: On page 3, line 21, the word *pass phase* should be written as *pass phrase*.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claim 18 is rejected under 35 U.S.C. 112 because the claimed invention is directed to a single means claim. A single means claim, i.e., where a means recitation does not appear in combination with another recited element of means, is subject to an undue breadth rejection under 35 U.S.C. 112, first paragraph. In re Hyatt, 708 F.2d 712, 714-715, 218 USPQ 195, 197(Fed. Cir. 1983)
A single means claim which covered every conceivable means for achieving the stated purpose was held nonenabling for the scope of the claim because the specification disclosed at most only those means known to the inventor. See MPEP § 2164.08 (a).

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claim 19 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 19 is directed to a computer-program product comprising software code for performing the steps of a key server. The recited limitation of a computer program does not meet the definition of statutory subject matter. The claimed elements instead appear to describe a mere arrangement of a computer program which constitutes non-functional descriptive material, and is therefore not statutory subject matter. See MPEP § 2106 IV.B.1.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-17 are rejected under 35 U.S.C. 102(e) as being anticipated by Kaplan et al. (US Patent No. 6,704,871).

Referring to the rejection of claim 1, Kaplan et al. discloses a method for storing keys for authentication or encryption, the method being carried out by a host system, and comprising the steps of:

the host system operating as a key server controlling storage of the keys in a software database file system (See Column 5, lines 17-20, Column 6, lines 40-50, and Column 74, lines 42-53)

Referring to the rejection of claim 2, Kaplan et al. discloses the claimed limitation wherein the key server manages separate and individual security for each key with per-key encryption (See Column 5, lines 21-35, 58-65)

Referring to the rejection of claim 3, Kaplan et al. discloses the claimed limitation wherein the key server associates a set of keys with an alias, and each alias, has an associated pass phrase (See Column 90, lines 56-58, Column 101, lines 13-15)

Referring to the rejection of claim 4, Kaplan et al. discloses the claimed limitation wherein a request to create a key is made by an alias, the server causes a key to be generated by a cryptographic accelerator, and stores the key in the database (See Column 130, lines 58-53)

Referring to the rejection of claim 5, Kaplan et al. discloses the claimed limitation wherein the key server signs and hashes all files, and then hashes them to signed and encrypted files (See Column 6, lines 61-67, Column 7, lines 1-29)

Referring to the rejection of claim 6, Kaplan et al. discloses the claimed limitation wherein aliases identify key rings which hold keys and certificates associated with the alias (See Column 69, lines 63-67, Column 70, lines 1-4)

Referring to the rejection of claim 7, Kaplan et al. discloses the claimed limitation wherein each key ring is an indexed structure (See Column 8, lines 18-27, Column 11, lines 29-35)

Referring to the rejection of claim 8, Kaplan et al. discloses the claimed limitation wherein each key ring allows access to certificate descriptions which refer to files and contain information on inception, dates, expiry dates, and creation dates (See Column 11, lines 29-35)

Referring to the rejection of claim 9, Kaplan et al. discloses the claimed limitation wherein the key server, upon deletion of a key, spawns a thread which writes zeros or random numbers into a file which contains the key to overwrite the key (See Column 93, lines 35-65)

Referring to the rejection of claim 10, Kaplan et al. discloses the claimed limitation wherein over-writing is performed a configurable plurality of times (See Column 91, lines 23-37)

Referring to the rejection of claim 11, Kaplan et al. discloses the claimed limitation wherein the accelerator creates a meta key (Km) and a salt (S) for access to the key server (See Column 39, lines 51-62)

Referring to the rejection of claim 12, Kaplan et al. discloses the claimed limitation wherein the key server negotiates a session key (Ks) with the

accelerator for a session, and the session key is deleted for a session (See Column 94, lines 60-65, Column 102, lines 21-31)

Referring to the rejection of claim 13, Kaplan et al. discloses the claimed limitation wherein the key server uses the session key to encrypt data (Rc) associated with a key-creation request, and transmits the encrypted data to the accelerator (See Column 130, lines 28-67, Column 131, lines 1-30)

Referring to the rejection of claim 14, Kaplan et al. discloses the claimed limitation wherein the management system manages a private key (Kp) of a public/private key pair as follows:

the accelerator hashes a pass phrase P with a salt S to produce a per-key encryption key (Kk),

the accelerator encrypts (Kp) with (Kk),

the accelerator encrypts the result with additional data (Km),

and the accelerator returning the result to the key server (See Column 92, lines 46-59, Column 93, lines 16-26, and Column 95, lines 14-40)

Referring to the rejection of claim 15, Kaplan et al. discloses the claimed limitation wherein the key server allows access to keys only if the requesting user is already associated with a stored key (See Column 102, lines 60-67)

Referring to the rejection of claim 16, Kaplan et al. discloses the claimed limitation wherein the management system carries out the following steps upon receiving a request from an alias for use of an existing key:

(a) the initial request is expressed in terms of P,

(b) the encrypted key is retrieved from the key store, and this is combined with P to form a request structure (Ru),

(c) (Ru) is encrypted with Ks and is transmitted to the accelerator,

(d) the accelerator decrypts (Ru) using (Ks),

(e) the key is decrypted with (Km),

(f) the passphrase from the request is hashed with S to give (Kk),

(g) and the result from step (e) is decrypted with (Kk) to give (Kp), the original key (See Column 5, lines 66-67, Column 6, lines 1-27, Column 39, lines 1-23, 51-67, Column 40, lines 1-19)

Referring to the rejection of claim 17, Kaplan et al. discloses the claimed limitation wherein the key server encrypts each key using a meta key associated with a accelerator, whereby a plurality of accelerators may use the key server (See Column 10, lines 55-63)

Conclusion

1. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Johnson et al. (US Patent No. 5,815,573) discloses a cryptographic key recovery system. Nordenstam et al. (US Patent No. 6,711,263) discloses a secure distribution and protection of encryption key information.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cdf
August 22, 2005

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER